UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,342	04/12/2001	David John Craft	AUS920010088US1	3785

50675 7590 02/17/2006

IBM CORP. (CLG)
c/o CARDINAL LAW GROUP
1603 ORRINGTON AVENUE
SUITE 2000
EVANSTON, IL 60201

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 02/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/833,342	**Applicant(s)** CRAFT ET AL.	
	Examiner Ponnoreay Pich	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claims 1-2 and 4-39 are pending. Claim 3 was cancelled.

Response to Amendment

Applicant's amendments have been noted. The 112, second paragraph rejection from the prior office action is withdrawn due to applicant's amendment. Also note new rejections presented below in response to the amendments.

Response to Arguments

Applicant argues as per claims 1 and 6 that Easter fails to disclose embedding a public cryptographic key. The examiner respectfully disagrees. Column 3, lines 58-63 of Easter discloses a programmable storage area on the chip system which is designated for storing a public key. Easter discloses that during operational initialization of the chip, the public key is loaded. This reads on embedding the public cryptographic key.

Applicant argues as per claims 1 and 6 that the examiner is mistaken in stating that because the public and private keys disclosed by Easter are different, they are not related by a cryptographic key pairing. The examiner respectfully disagrees. The examiner would like to emphasize that the limitation in contention states that the public cryptographic key and the private cryptographic key are not related by **a** cryptographic key pair relationship. This is not the same thing as the public and private cryptographic key not being related by **any** cryptographic key pair relationship. The public and private key disclosed by Easter may be related in that they have an asymmetrical cryptographic public/private key pair relationship, however, by that very nature, it prohibits the two keys from having other types of cryptographic key pair relationships. For example, in symmetrical encryption, a sender has one key and a receiver has another key. Both these keys are related by a cryptographic key pair relationship in that both keys have the same key values. Since the keys disclosed by Easter are public and private keys, the keys are not the same value, thus cannot have the type of cryptographic key pair relationship they would have if a symmetric key system was disclosed instead. Another type of cryptographic key pair relationship between two keys is where two keys are related in that they are each part of another key (i.e. see US 2002/0076042 or US 6,975,727). The public and private keys disclosed by Easter also does not have this type of cryptographic key pair relationship. The examiner believes that applicant may have meant for the limitation being argued to only refer to cryptographic key pair relationships in regards to asymmetric cryptography (i.e. a public/private key pair relationship) as disclosed in the specification, but although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The examiner notes that claims 6-9 were not amended. The rejections of these claims are repeated below for record.

The rest of applicant's amendments are in regards to amended limitations and dependency. These arguments are moot in view of new rejections presented below.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

> art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 10-39 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Amended claims 10,13, 16, 19, 21, 23, 25, 27, 29, 31, 34, and 37 have been amended to include the limitation that a client public key is stored exclusively outside the client. The examiner respectfully submits that this limitation is new matter as it would not have been clear to one of ordinary skill in the art from applicant's specification and drawings that applicant's invention had this limitation. The examiner notes that Fig 2 shows a client which does not show a client public key stored in the client. However, this is not the same thing as prohibiting the client public key from being stored in the client so that the client public key is stored **exclusively** outside the client. The examiner submits this limitation is a pretty major and definite limitation and absent any explicit disclosure of the limitation in the specification, one of ordinary skill would be more likely to interpret the drawing as conveying only that which is necessary to understand the claimed invention and any unnecessary details are not shown rather than the limitation that applicant is now trying to claim in the amended claims. Any claims not specifically addressed are rejected by virtue of dependency.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-2 and 4-5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 1 recites "an associated serial number" in lines 1-2. It is unclear what the serial number is associated with. The examiner will apply broadest, reasonable interpretation to the claim and assume anything can be associated with the serial number.
2. Claim 1 recites "the serial number" in the last line, which lacks antecedent basis. It is unclear if the serial number refers to the associated serial number earlier recited or a different serial number.
3. Any claims not specifically addressed are rejected by virtue of dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 6-8 are rejected under 35 U.S.C. 102(b) as being anticipated by Easter et al (U.S. 5,559,889).

Claim 6:

Easter et al disclose an article of manufacture comprising:

1. A first read-only memory structure containing an embedded private cryptographic key (col 2, lines 35-41).
2. A second read-only memory structure containing an embedded public cryptographic key, wherein the public cryptographic key and the private cryptographic key are not related by a cryptographic key pair relationship (col 2, lines 35-41).

The examiner has interpreted claim 6 as broadly as reasonable and determined that it is possible that the first and second memory structure can be the same structure.

Claim 7:

Easter et al disclose an article of manufacture of claim 6 wherein the article of manufacture is a semiconductor chip (col 2, lines 35-41). An integrated circuit chip is inherently the same thing as a semi-conductor chip.

Claim 8:

Easter et al disclose an article of manufacture of claim 7 wherein the semiconductor chip is capable of providing interface processing at a client (col 4, lines 21-31).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Easter et al (U.S. 5,559,889) in view of ecommerce-guide.com ("A Framework For SmartCard Payment Systems – Part One" by Mark Merkow, June 22, 2000).

Claim 9:

Easter et al failed to disclose an article of manufacture of claim 8 wherein the first read-only memory structure and the second read-only memory structure are contained within a cryptographic unit of a CPU chip. However, ecommerce.com discloses a single chip configuration which has a CPU, ROM, and a cryptographic unit ("Just What Are SmartCards?", line 1 and "Chip Families"). Ecommerce.com disclosed that a cryptographic co-processor could be added to the CPU for applications which require faster execution of cryptographic algorithms. Easter et al disclosed that their invention could be used in both a corporate and government environment. As such, though security is a major issue, so is the speed at which communication occur as the longer it takes for a client and server to communicate, the more costly the communication can become. Thus, one of ordinary skill in the art at the time of the applicant's invention would be motivated to combine Easter et al's teachings with ecommerce.com's teaching of a single integrated circuit chip with built in read-only memory (to store the public and private keys) and a cryptographic co-processor unit to create a system that is both secure and allows for faster communication.

Claims 1, 2, 4-5, 10, 13, 16, 19, 21, 23, 31, 34, 37, 32, 35, 38, 33, 36, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Davis (US 5,970,147).

Claim 1:

Arnold discloses:

1. Selecting a private cryptographic key (col 2, lines 9-24).
2. Selecting a public cryptographic key, wherein the public cryptographic key and the private cryptographic key are not related by a cryptographic key pair relationship (col 2, lines 9-24).
3. Embedding the private cryptographic key and the public key in read-only memory on the semiconductor chip (col 4, lines 1-24).

Arnold does not explicitly disclose also embedding the serial number in read-only memory on the semiconductor chip. However, Davis discloses embedding the serial number in read only memory on the semiconductor chip (col 1, line 67-col 2, line 4 and col 4, lines 26-39). Davis discloses that at the time applicant's invention was made, one of the disadvantages that would be realized in cryptography is that as cryptographic techniques become more advanced, larger, more costly packages will be required because larger amounts of non-volatile/read-only device memory will be necessary to store greater amounts of cryptographic information. Davis discloses that it would be more cost efficient to mitigate the amount of memory placed on a cryptographic device, i.e. semi-conductor chip, (col 1, lines 37-50). Davis discloses that embedding a serial number in read-only memory would allow some of the cryptographic information that would normally be placed in a device's read-only memory to be moved from the device's memory since the serial number could be used as an index for a table of pointers in a database containing the majority of cryptographic information (col 1, lines 22-54).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Arnold's invention using Davis's teachings according to the limitations recited in claim 1. One of ordinary skill would have been motivated to do so because Davis's teachings would allow one to reduce the amount of information stored in a cryptographic device's memory, thus reducing costs associated with the cryptographic device. Note Arnold was concerned with cost savings (col 6, lines 16-18).

The examiner further take official notice that embedding a serial number in read-only memory of a semiconductor chip is well known in the art even without Arnold's teachings. Because of this, it would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to modify Arnold's invention such that the semiconductor chip also had a serial number embedded in read-only memory. One of ordinary skill would have been motivated to do so because it would allow the chip and the keys associated with the chip to be uniquely identified.

Claim 2:

Arnold further discloses wherein the semiconductor chip provides interface processing at a client (col 4, lines 18-22).

Claim 4:

Davis further discloses storing the public cryptographic key in a database in association with the serial number (col 4, lines 26-39 and col 5, lines 58-62).

Claim 5:

Arnold further discloses wherein the private cryptographic key, and the public cryptographic key in the read-only memory are inaccessible to an input/output connection of the semiconductor chip (col 4, lines 36-40).

Claims 10, 13, and 16:

As per claim 10, Arnold discloses:

1. Generating a client message at the client (col 2, lines 9-24).
2. Retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a cryptographic key pair relationship, the embedded client private key being associated with a client public key (col 2, lines 9-24 and col 4, lines 14-24).

3. Encrypting the client message with the embedded server public key (col 2, lines 9-24).
4. Storing the encrypted client authentication data in the client message (col 2, lines 9-24).

Arnold does not explicitly disclose the client public key stored exclusively outside the client. This is implied by Arnold though (col 2, lines9-24). Elements A and B exchange their public keys and retain their own private keys, which reads on the client's public key being exclusively stored outside the client since the client does not keep a copy of its own public key. Note that elements A and B can both be a client or a server. Further, Davis discloses storing the client public key exclusively outside the client (col 1, line 67-col 2, line 4 and col 4, lines 26-39). At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Arnold's invention according to the limitations recited in claim 10 in light of Davis's teachings. One of ordinary skill would have been motivated to do so because by not storing the client's public key inside the client, less memory would be needed at the client, thus reducing costs associated with the client. Note Arnold was concerned with cost savings (col 6, lines 16-18).

Claims 13 and 16 are substantially similar to claim 10. Claim 13 is directed towards an apparatus with means for implementing the method of claim 10. Claim 16 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 10. Claims 13 and 16 are rejected for the same reasons given in claim 10.

Claims 19, 21, and 23:

As per claim 19, Arnold discloses:

1. Generating a server message at the server (col 2, lines 9-24).
2. Retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client (col 2, lines 9-24).
3. Encrypting the server message with the client public key (col 2, lines 9-24).
4. Sending the server message to the client (col 2, lines 9-24).

Arnold does not explicitly disclose:

1. Retrieving information that was requested by the client.
2. Storing the retrieved information in the server message.

However, the examiner take official notice that the above limitations were well known in the art at the time applicant's invention was made. It would have been obvious to one of ordinary skill in the art to modify Arnold's invention such that the server retrieved information that was requested by the client and store the retrieved information in the server message that is sent to the client. One of ordinary skill would have been motivated to do so because this is essentially how a client-server relationship works, i.e. a client request information being "served" by a server, the server retrieves the requested information, and sends the requested information to the client via a server message to the client if the client is authorized to receive that information.

Arnold also does not explicitly disclose the client public key is stored exclusively outside the client. This is implied by Arnold though (col 2, lines 9-24). Elements A and B exchange their public keys and retain their own private keys, which reads on the client's public key being exclusively stored outside the client since the client does not keep a copy of its own public key. Note that elements A and B can both be a client or a server. Further, Davis discloses the client public key is stored exclusively outside the client, i.e. cryptographic device (col 4, lines 43-45 and 50-54).

At the time applicant's invention was made, it would have been obvious to one ordinary skill in the art to further modify Arnold's invention such that the client public key is stored exclusively outside the client. One of ordinary skill would have been motivated to do so as it would allow a reduction in the amount of memory needed at the client, thus reducing costs associated with the client. Note Arnold was concerned with cost savings (col 6, lines 16-18).

Claims 21 and 23 are substantially similar to claim 19. Claim 21 is directed towards an apparatus with means for implementing the method of claim 19. Claim 23 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 19. Claims 21 and 23 are rejected for the same reasons given in claim 19.

Claims 31, 34, and 37:

As per claim 31, Arnold discloses:

1. Receiving a server message from the server (col 2, lines 9-24).
2. Retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key (col 2, lines 9-24 and col 4, lines 14-24).
3. Decrypting the server message with the embedded client private key (col 2, lines 9-24).

Arnold does not explicitly disclose the client public key is stored exclusively outside the client. This is implied by Arnold though (col 2, lines9-24). Elements A and B exchange their public keys and retain their own private keys, which reads on the client's public key being exclusively stored outside the client since the client does not keep a copy of its own public key. Note that elements A and B can both be a client or a server. Further, Davis discloses storing the client public key exclusively outside the client (col 1, line 67-col 2, line 4 and col 4, lines 26-39). At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Arnold's invention according to the limitations recited in claim 31 in light of Davis's teachings. One of ordinary skill would have been motivated to do so because by not storing the client's public key inside the client, less memory would be needed at the client, thus reducing costs associated with the client. Note Arnold was concerned with cost savings (col 6, lines 16-18).

Claims 34 and 37 are substantially similar to claim 31. Claim 34 is directed towards an apparatus with means for implementing the method of claim 31. Claim 37 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 31. Claims 34 and 37 are rejected for the same reasons given in claim 31.

Claims 32, 35, and 38:

As per claim 32, Arnold further discloses retrieving encrypted server authentication data from the server message; retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client; decrypting the server authentication data with the embedded server public key; and verifying the decrypted server authentication data (col 2, lines 25-41).

Claims 35 and 38 are substantially similar to claim 32. Claim 35 is directed towards an apparatus with means for implementing the method of claim 32. Claim 38 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 32. Claims 35 and 38 are rejected for the same reasons given in claim 32.

Claims 33, 36, and 39:

As per claim 31, Arnold does not explicitly disclose retrieving requested information from the server message; and in response to a determination that the decrypted server authentication data was verified, processing the requested information. However, examiner asserts these limitations were well known in the art at the time applicant's invention was made and describes a typical client-server relationship. A client typically requests information from a server, the server receives the requests, and if the client is authorized to receive the information, the server sends the information to the client who receives the requested information via the server's reply message. The client typically only processes the requested information if the decrypted server authentication data was verified for security purposes.

At the time applicant's invention was made, it would have been obvious to further modify Arnold's invention according to the limitations recited in claim 33. One of ordinary skill would have been motivated to do so because the limitations recited in claim 33 describes a typical client-server relationship.

Claims 36 and 39 are substantially similar to claim 33. Claim 36 is directed towards an apparatus with means for implementing the method of claim 33. Claim 39 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 33. Claims 36 and 39 are rejected for the same reasons given in claim 33.

Claims 11, 14, 17, 12, 15, 18, 20, 22, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Davis (US 5,970,147) and further in view of Sandhu et al (US 2002/0078344).

Claims 11, 14, and 17:

As per claim 11, Arnold further discloses:

1. Retrieving client authentication data (col 3, lines 1-13).
2. Retrieving the embedded client private key from a read-only memory structure in an article of manufacture in the client (col 2, lines 25-41).

Arnold does not explicitly disclose:

1. Encrypting the client authentication data with the embedded client private key.
2. Storing the encrypted client authentication data in the client message.

However, Sandhu discloses retrieving client authentication data; encrypting the client authentication data with the embedded client private key; and storing the encrypted client authentication data in a client message (p3, paragraph 28).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Arnold's invention according to the limitations recited in claim 11. One of ordinary skill would have been motivated to do so because the client-side-authentication technique disclosed by Sandhu would make communication between a client and a server more secure.

Claims 14 and 17 are substantially similar to claim 11. Claim 14 is directed towards an apparatus with means for implementing the method of claim 11. Claim 17 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 11. Claims 14 and 17 are rejected for the same reasons given in claim 11.

Claims 12, 15, and 18:

As per claim 12, Davis further discloses:

1. Retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client (col 4, lines 26-33; col 5, lines 58-62; and col 6, lines 27-29).
2. Storing a copy of the embedded client serial number in the client message (col 5, lines 58-62 and col 6, lines 27-29).

Claims 15 and 18 are substantially similar to claim 12. Claim 15 is directed towards an apparatus with means for implementing the method of claim 12. Claim 18 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 12. Claims 15 and 18 are rejected for the same reasons given in claim 12.

Claims 20, 22, and 24:

As per claim 20, Arnold discloses:

1. Retrieving server authentication data (col 3, lines 1-13).
2. Retrieving a server private key (col 2, lines 25-41).

Arnold does not explicitly disclose encrypting the server authentication data with the server private key; and storing the encrypted server authentication data in the server message.

However, Sandhu discloses retrieving server authentication data; encrypting the server authentication data with the server private key; and storing the encrypted server authenticate data in the server message (p3, paragraph 27). At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Arnold's invention according to the limitations recited in claim 20 in light of Sandhu's teachings. One of ordinary skill would have been motivated to do so because the server-side-authentication disclosed by Sandhu would make communication between a client and a server more secure.

Claims 22 and 24 are substantially similar to claim 20. Claim 22 is directed towards an apparatus with means for implementing the method of claim 20. Claim 24 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 20. Claims 22 and 24 are rejected for the same reasons given in claim 20.

Claims 25, 27, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Easter et al (US 5,559,889) and further in view of Davis (US 5,970,147).

Claims 25, 27, and 29:

As per claim 25, Arnold discloses:

1. Receiving a client message from the client (col 2, lines 9-24).
2. Retrieving a server private key (col 2, lines 9-24).
3. Decrypting the client message with the server private key (col 2, lines 9-24).

4. Retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client (col 2, lines 9-24 and col 4, lines 14-24).
5. Wherein the read-only memory structure has an embedded server public key, the embedded server public key and the embedded client private key not being related by a cryptographic key pair relationship (col 2, lines 9-24 and col 4, lines 9-24).

Arnold does not disclose retrieving a client serial number from a decrypted client message. Arnold does not disclose the client public key is associatively stored and retrieved with the retrieved client serial number. Arnold does not explicitly disclose the client public key is stored exclusively outside the client. However, Arnold does imply the client public key is stored exclusively outside the client (col 2, lines 9-24). Elements A and B exchange their public keys and retain their own private keys, which reads on the client's public key being exclusively stored outside the client since the client does not keep a copy of its own public key.. Note that elements A and B can both be a client or a server.

However, the examiner asserts that clients embedding the client's serial number in an encrypted client message and a receiver retrieving the client serial number from a decrypted client message was well known in the art at the time applicant's invention was made. For instance, when a message is sent, the id of the sender is usually attached to the message to identify the sender of the message. This id reads on the client's serial number embedded in the client's message. When the receiver of the message replies to the sender/client, this id allows the receiver to know who to reply to (i.e. the reply to field of an email address). Easter also discloses a serial number is associated with a public key, the public key is associatively stored and retrieved with the serial number (col 5, line 63-col 6, line 3). At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Arnold's invention to retrieve a client serial number from a decrypted client message and use that retrieved client serial number to retrieve a client public key that is associatively stored with the client serial number. One of ordinary skill would have been motivated to do so because it would allow a server to securely communicate with multiple clients using each client's specific public key.

Further, Davis discloses the client public key is stored exclusively outside the client, i.e. cryptographic device (col 4, lines 43-45 and 50-54). One of ordinary skill would have been motivated to store the client's public key in Arnold's modified invention exclusively outside the client because it would allow a reduction in the amount of memory needed at the client, thus reducing costs associated with the client. Note Arnold was concerned with cost savings (col 6, lines 16-18).

Claims 27 and 29 are substantially similar to claim 25. Claim 27 is directed towards an apparatus with means for implementing the method of claim 25. Claim 29 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 27. Claims 27 and 29 are rejected for the same reasons given in claim 25.

Claims 26, 28, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Easter et al (US 5,559,889) further in view of Davis (US 5,970,147) and further in view of Sandhu et al (US 2002/0078344).

Claims 26, 28, and 30:

As per claim 26, Arnold does not explicitly disclose retrieving encrypted client authentication data from the client message; decrypting the client authentication data with the retrieved client public key; and verifying the decrypted client authentication data.

However, Sandhu discloses retrieving encrypted client authentication data from the client message; decrypting the client authentication data with the retrieved client public key; and verifying the decrypted client authentication data (p3, paragraph 28).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Arnold's invention according to the limitations recited in claim 26. One of ordinary skill would have been motivated to do so because the client-side-authentication technique disclosed by Sandhu would make communication between a client and a server more secure.

Claims 28 and 30 are substantially similar to claim 26. Claim 28 is directed towards an apparatus with means for implementing the method of claim 26. Claim 30 is directed towards a computer program product in a computer-readable medium comprising instructions for implementing the method of claim 26. Claims 28 and 30 are rejected for the same reasons given in claim 26.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100